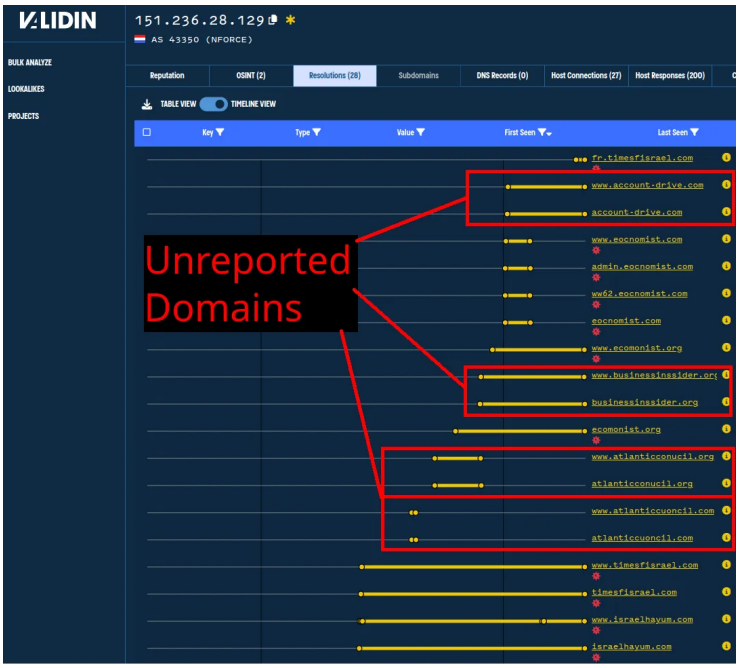
Expanding APT42 Intelligence with Validin

⋮ 5/3/2024



By: Kenneth Kinion

2024-05-03

Introduction

In this blog post, we'll use indicators from a recent threat report as a starting point for further enrichment in the Validin platform to find additional likely-related infrastructure.

On May 1, 2024, Mandiant published a threat report detailing the activities and techniques used by APT42, an Iranian state-sponsored cyber espionage actor. The Mandiant team provided 148 domains in the Virus Total collection included with the report. The threat report detailed websites that:

- Pose as legitimate services, news outlets, and NGOs
- Imitate login pages from reputable technology companies
- Poste as "mailer daemons"
- Pose as URL shortening services

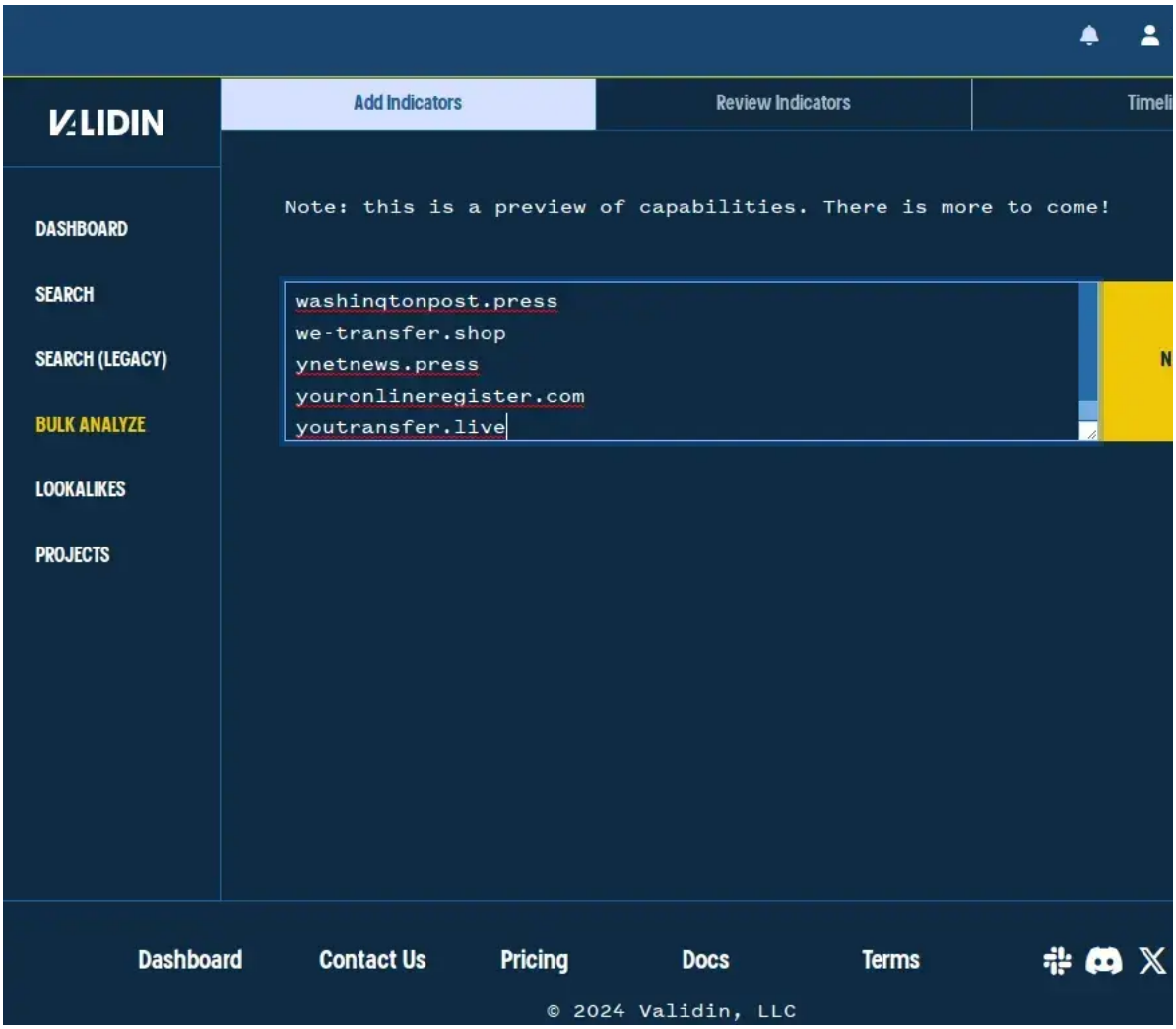
The threat actor uses this infrastructure to assist with credential harvesting and malware deployment.

Let's see what else we can find with Validin!

Initial Bulk Enrichment

Given the relatively large starting point, we'll use Validin's bulk search feature, which is available to all Professional and Enterprise users and designed to assist with bulk analysis workflows.

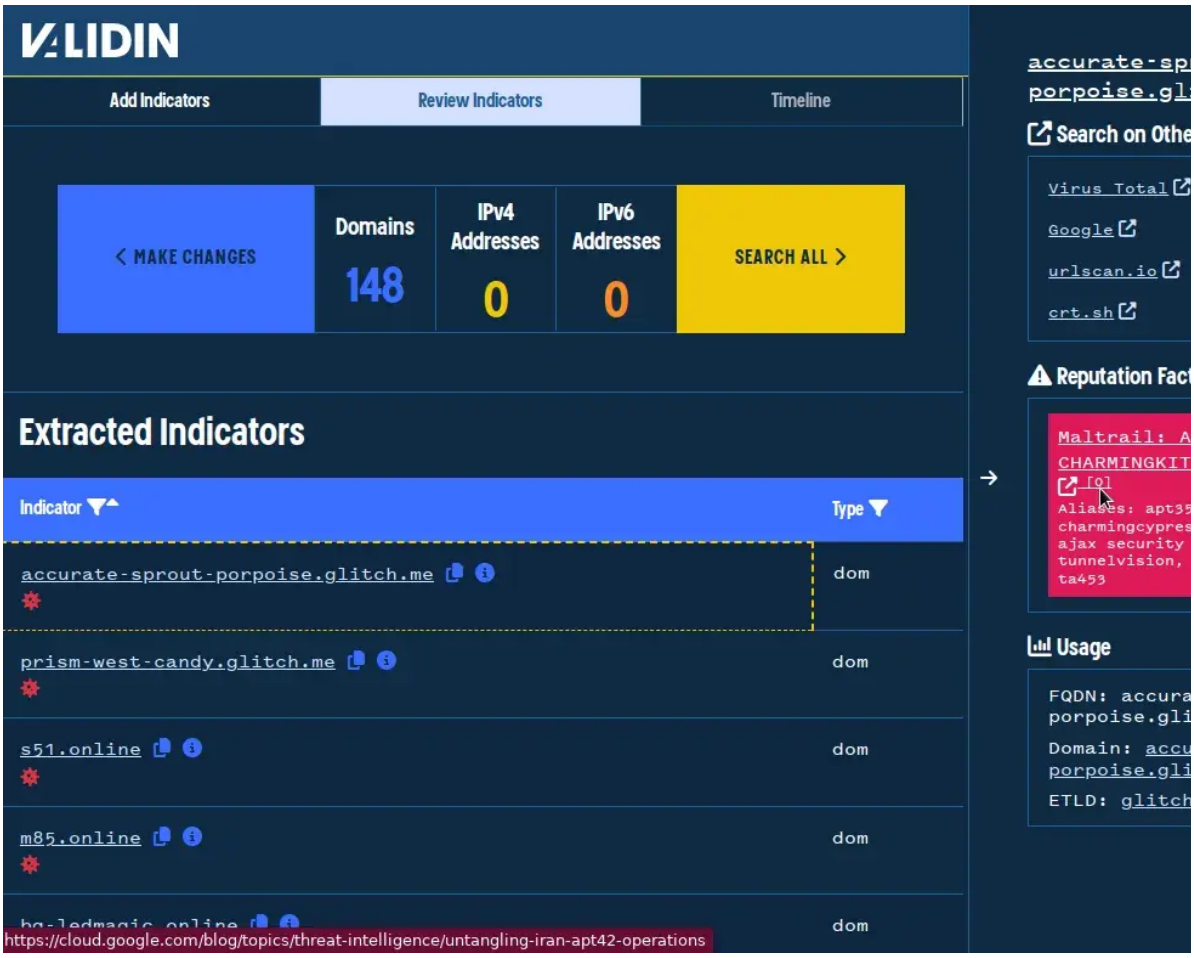
We start by copying the indicators from the Virus Total collection into the indicators text box:



Copying indicators from a threat report into Validin's bulk analysis textbox.

Note: the Mandiant team did a great job organizing these indicators by usage, and that would be a great way to work through collections to find related behavior. However, we'll enrich all indicators in this post at once for brevity.

Upon clicking "Next," we notice that every indicator on the list has already been tagged as malicious by Validin. This is because these indicators were added to the Maltrail project shortly after the report was published. Validin includes a direct link to both the source report and the Maltrail project, which contains indicators from other published research from APT42.

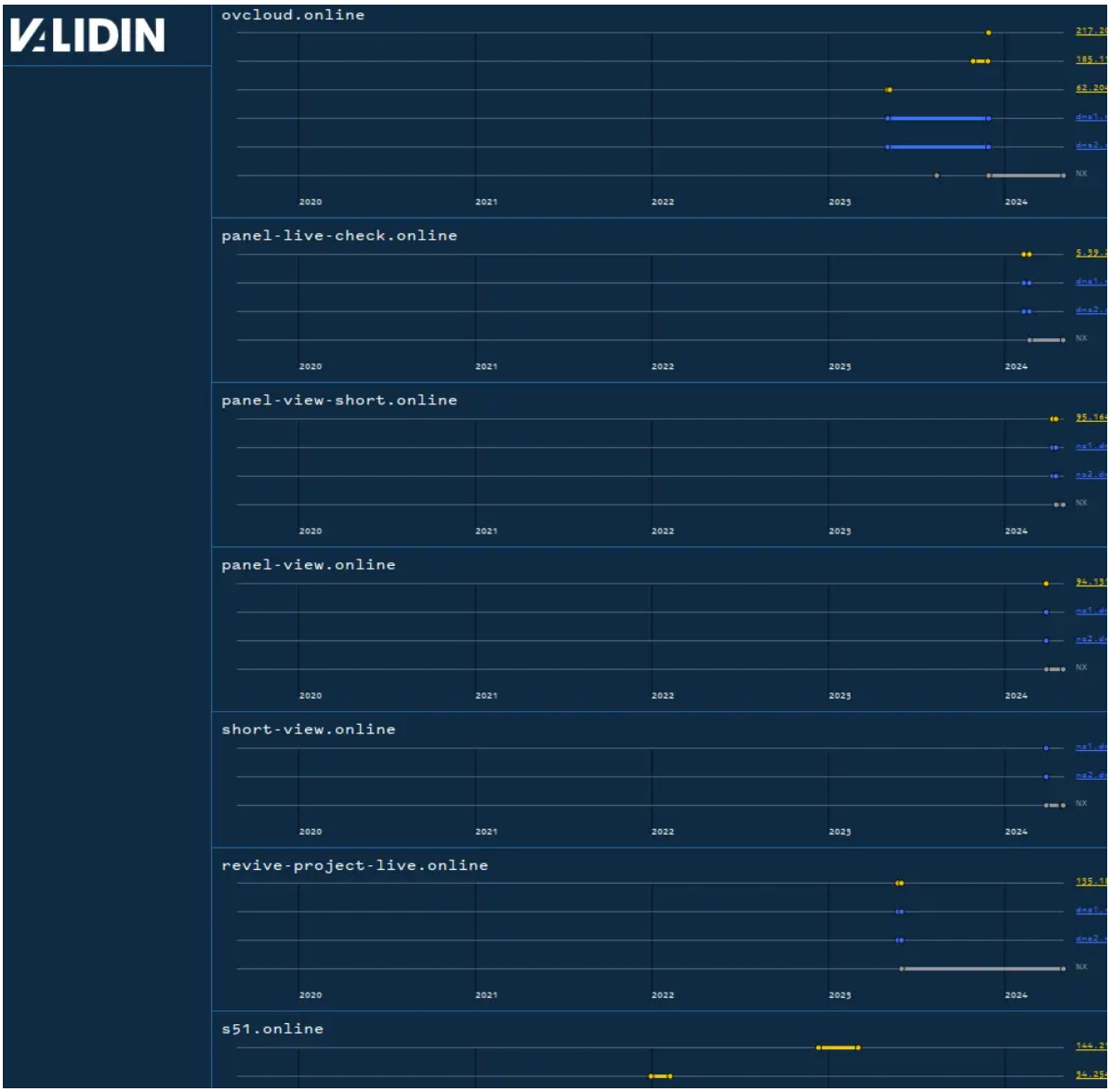


Validin provides direct links to reported threat intelligence sources whenever possible.

By clicking “Search All,” Validin performs DNS queries against all supplied indicators and then displays a side-by-side activity timeline for every domain in the initial report. From this view, we can begin iterating and expanding awareness of additional likely actor-controlled infrastructure.

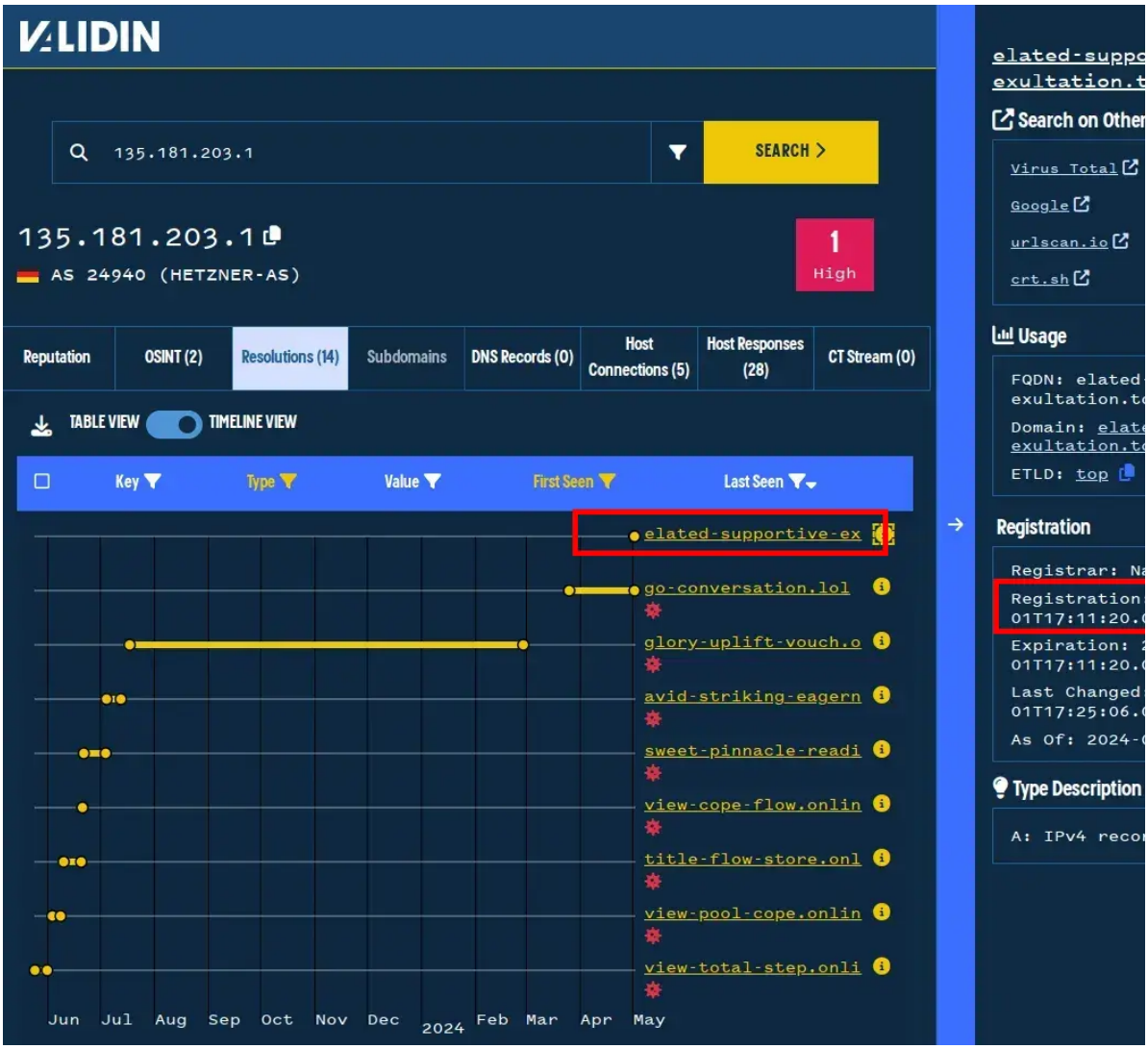
Identifying Hosting Patterns

The first thing I notice when looking at the hosting patterns is that the activity timelines do not line up very uniformly. Indeed, Mandiant reports that one cluster of domains has been active since 2019, another since 2021, and another since 2022. Even within these clusters, domain activity is not tightly coordinated on the time scale.



Many domains are only active very briefly and during non-overlapping time windows.

Some of the IP addresses show up multiple times. A few are parking or cloud proxies (like Cloudflare), but others have a fairly limited history. After time filtering, we see some patterns like the following:



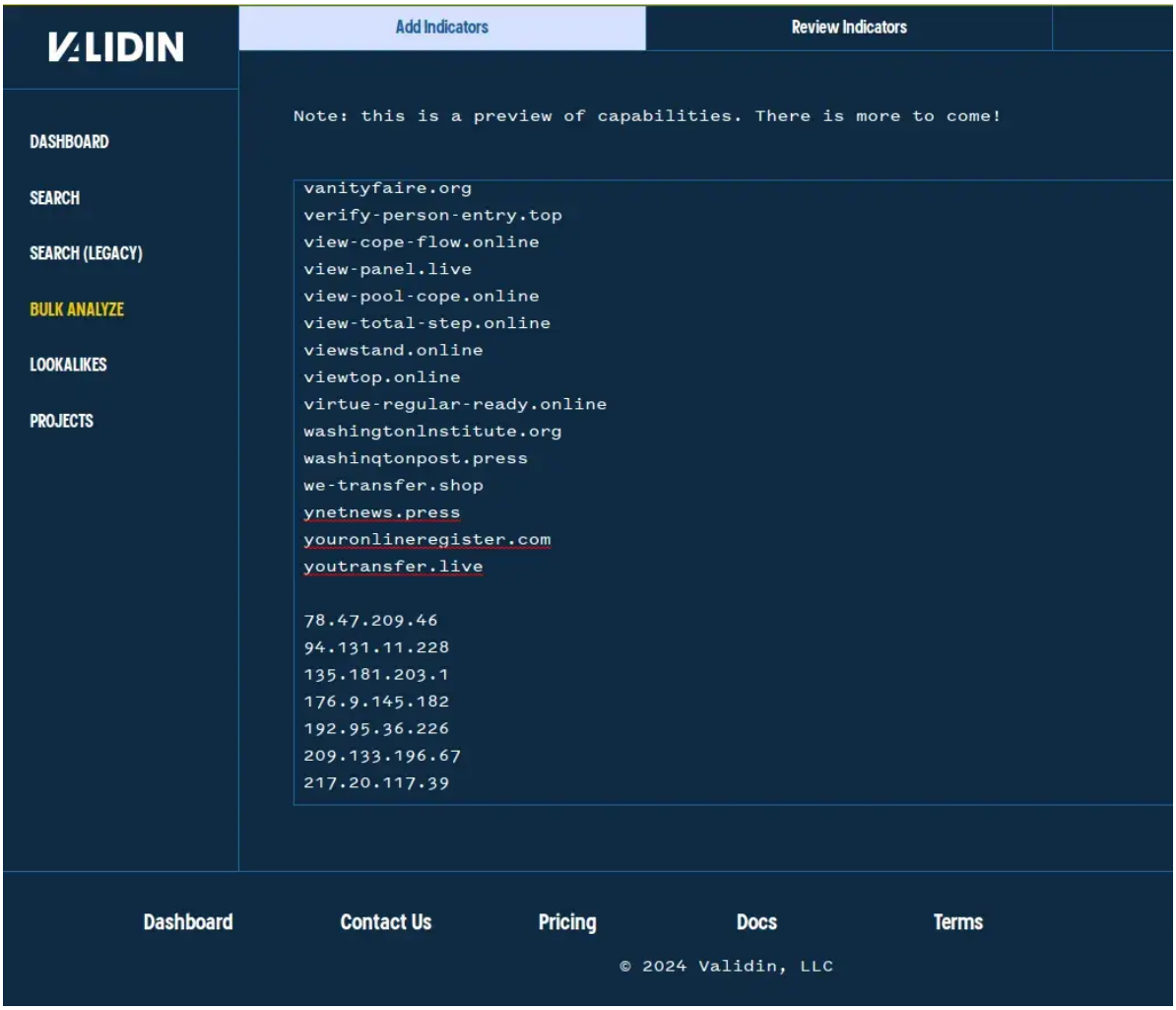
IP history shows many domains used for relatively brief and non-overlapping periods.

On my first pivot, I see a domain that isn't highlighted as known-malicious by Maltrail, like elated-supportive-exultation[.]top pivoting through 135.181.203[.]1. That domain was registered the same day the Mandiant report was published, so we've used Validin to find bleeding-edge indicators.

Continuing this process, I build a short list of IP addresses that look like they'll provide good pivots:

```
78.47.209[.]46
94.131.11[.]228
135.181.203[.]1
176.9.145[.]182
192.95.36[.]226
209.133.196[.]67
217.20.117[.]39
```

Then I add those indicators back to the the bulk search list (under "Add Indicators") to re-run the bulk analysis workflow:

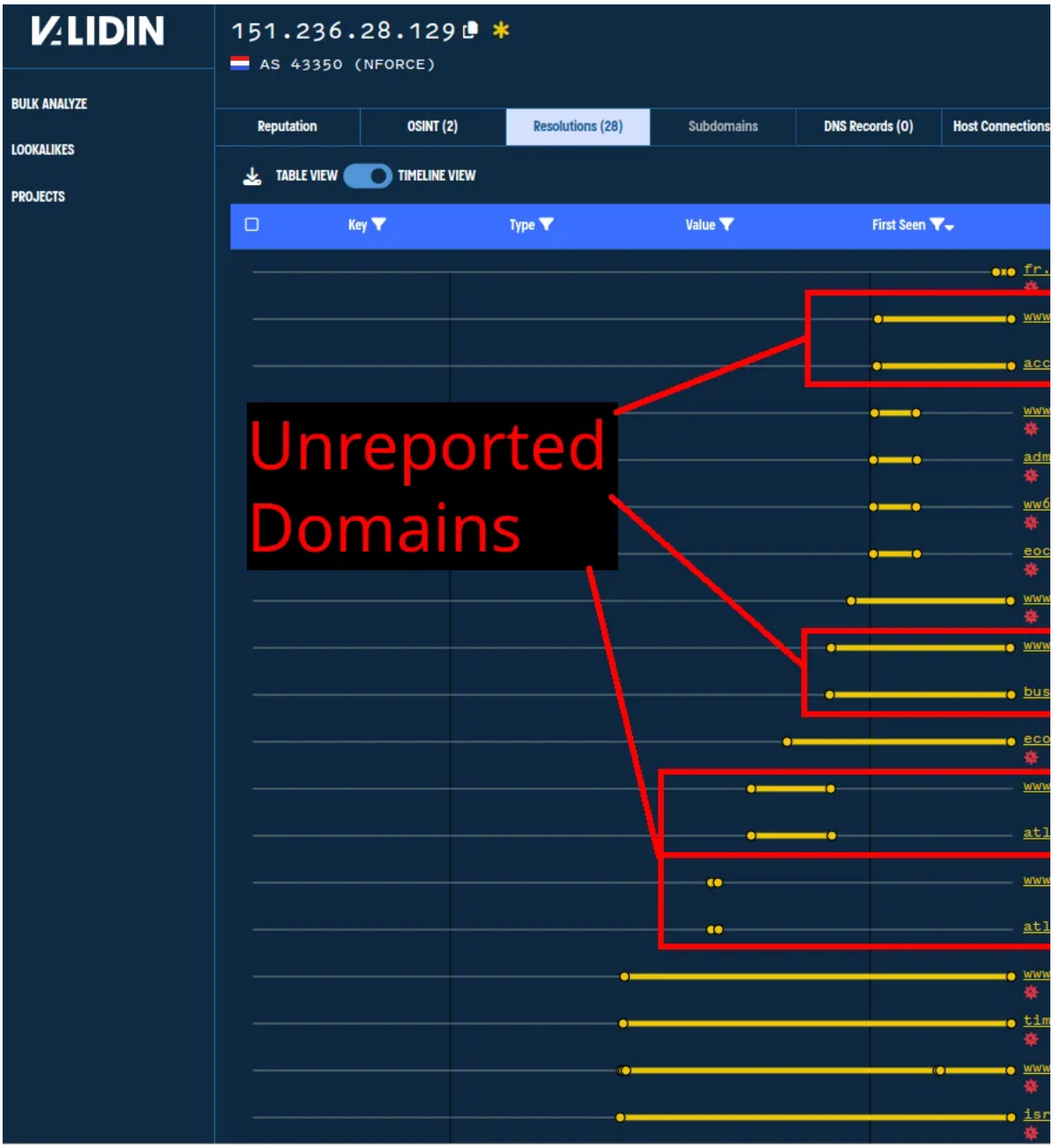


Adding IP indicators to the bulk search list.

This will enable two things:

1. I'll be able to visualize the potential pivots on the timeline view quickly
2. I'll be able to see, in the timeline view, which indicators I've already added as pivots

Some of the IPs are a goldmine of new indicators:



Finding unreported domains through PDNS pivots using IP hosting history.

The PDNS history for `209.133.196[.]67` shows domains with similar short-lived usage patterns, naming conventions, and themes to other domains in the ground truth clusters.

After adding new indicators to the start of the bulk analysis workflow, I re-run the workflow to look for domains or IPs that I can reasonably assume to be part of the same cluster of activity.

Enrichment Additions

After several iterations of this process, I've added 77 additional effective second-level domains (E2LDs) that I have reasonable confidence are related based on the patterns revealed in their PDNS history. I've also added 39 IP addresses that the threat actor appears to have had control over at one point or another.

Conclusion

The Validin platform facilitates threat research and validation through an easy-to-navigate UI, bulk analysis features, and deep, precise DNS history. This combination enables researchers to quickly learn about domain and IP history, understand activity patterns, and discover new infrastructure.

Ready to take your threat intelligence program to the next level? Validin is your answer. Contact us to explore our enterprise options and discover how Validin can affordably empower your threat intelligence team.

```
permission-data.online
meeting-share[.]online
files-archive[.]online
share-meeting[.]online
modification-check[.]online
direction-check[.]online
allow-permission[.]online
15248636[.]site
activity-179384736[.]site
web-getdata[.]site
jubilatesee[.]site
online-meeting[.]site
short-modification[.]site
direction-session-verify[.]site
france24[.]live
videocallservice[.]live
paneling-check-live[.]live
paneling-cheking-df[.]live
pnael-checking[.]live
shorting-urling[.]live
short-urling[.]live
shorturling[.]live
3dauth[.]live
shortoni[.]live
conferencecall[.]live
panel-status-join[.]live
confirm-validation.mywire[.]org
gatestonelnstitute[.]org
atlanticconucil[.]org
continue-recognized.hopto[.]org
review-session.hopto[.]org
session-review.hopto[.]org
confirmation-verify.hopto[.]org
confirm-validity.hopto[.]org
businessinssider[.]org
responsiblestatcraft[.]org
safeshortl[.]ink
clarification[.]network
products-services[.]network
accredit[.]network
recognize-validation.theworkpc[.]com
accounts-drive[.]com
account-drive[.]com
atlanticcuoncil[.]com
drive-signin[.]com
account-siqnin[.]com
confirm-verify.servepics[.]com
tinurls[.]com
drive-acconuts[.]com
drive-account[.]com
drive-acconut[.]com
centrallibrary[.]info
elated-supportive-exultation[.]top
un-call[.]services
continue-recognized.ddns[.]net
eatonthehotground.ddns[.]net
schoolofpinkmice.ddns[.]net
identifier-service.ddns[.]net
verify-corroborate.ddns[.]net
digitalpufferfish.ddns[.]net
validation-confirm.ddns[.]net
flowerskindergarten.ddns[.]net
identity-session.ddns[.]net
confirm-validation.ddns[.]net
oceanofinformation.ddns[.]net
confirm-direction.ddns[.]net
strainitiatives.ddns[.]net
```

```
identifier-direct.ddns[.]net
ourredbucket.ddns[.]net
validity-accredit.ddns[.]net
thefireisburnt.ddns[.]net
africanblackwidow.ddns[.]net
modification-verify.ddns[.]net
identifier-verify.ddns[.]net
direction-veracity.ddns[.]net
accredit-validity.ddns[.]net
confirm-integrity.ddns[.]net
5.39.216[.]110
62.204.58[.]40
138.124.184[.]240
101.99.94[.]50
149.56.179[.]250
135.181.203[.]1
62.204.58[.]41
185.141.63[.]51
216.194.165[.]171
185.110.190[.]91
185.110.190[.]102
95.164.116[.]122
146.0.74[.]232
62.204.58[.]42
216.194.165[.]52
135.181.17[.]82
176.9.145[.]182
146.0.74[.]233
66.151.40[.]83
136.243.236[.]93
144.217.139[.]134
62.204.58[.]44
192.64.117[.]164
66.151.40[.]84
5.39.218[.]85
204.12.216[.]126
192.95.36[.]226
78.47.209[.]46
5.39.218[.]86
151.236.14[.]137
209.133.196[.]67
94.131.11[.]228
158.69.7[.]158
95.169.196[.]78
5.39.216[.]109
151.236.28[.]129
217.20.117[.]39
209.133.196[.]69
216.194.165[.]99
```